GlobalResearch
Center for Research on Globalization

Forensic Methodology Report: How to Catch Israel's NSO Group's Pegasus

By Amnesty International
Global Research, July 19, 2021
Amnesty International 18 July 2021

Theme: Intelligence

***

Introduction

The [Israel based] NSO Group [surveillance group] claims that its Pegasus spyware is only used to "investigate terrorism and crime" and "leaves no traces whatsoever".

This Forensic Methodology Report shows that neither of these statements are true. This report accompanies the release of the Pegasus Project, a collaborative investigation that involves more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories with technical support of Amnesty International's Security Lab.[1]

Amnesty International's Security Lab has performed in-depth forensic analysis of numerous mobile devices from human rights defenders (HRDs) and journalists around the world. This research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using [Israel's] NSO Group's Pegasus spyware.

As laid out in the UN Guiding Principles on Business and Human Rights, NSO Group should urgently take pro-active steps to ensure that it does not cause or contribute to human rights abuses within its global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs and journalists do not continue to become targets of unlawful surveillance.

In this Forensic Methodology Report, Amnesty International is sharing its methodology and publishing an open-source mobile forensics tool and detailed technical indicators, in order to assist information security researchers and civil society with detecting and responding to these serious threats.

This report documents the forensic traces left on iOS and Android devices following targeting with the Pegasus spyware. This includes forensic records linking recent Pegasus infections back to the 2016 Pegasus payload used to target the HRD Ahmed Mansoor.

The Pegasus attacks detailed in this report and accompanying appendices are from 2014 up to as recently as July 2021. These also include so-called “zero-click” attacks which do not require any interaction from the target. Zero-click attacks have been observed since May 2018 and continue until now. Most recently, a successful “zero-click” attack has been observed exploiting multiple zero-days to attack a fully patched iPhone 12 running iOS 14.6 in July 2021.

Sections 1 to 8 of this report outline the forensic traces left on mobile devices following a Pegasus infection. This evidence has been collected from the phones of HRDs and journalists in multiple countries.

Finally, in section 9 the report documents the evolution of the Pegasus network infrastructure since 2016. NSO Group has redesigned their attack infrastructure by employing multiple layers of domains and servers. Repeated operational security mistakes have allowed the Amnesty International Security Lab to maintain continued visibility into this infrastructure. We are publishing a set of 700 Pegasus-related domains.

Names of several of the civil society targets in the report have been anonymized for safety and security reasons. Individuals who have been anonymized have been assigned an alphanumeric code name in this report.

To read the full article by Amnesty International click here

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Featured image is from Howie Shia/Amnesty International

Articles by: Amnesty International